April 14, 2015

19th Annual FOCI Conference

Defense Security Service

STAN SIMS

DSS Director

Maintaining U.S. Advantage in National Security

"Economic Security is National Security"

LTG Robert Gard, PhD, USA (ret)
Chairman of the Center for Arms Control and Non-Proliferation

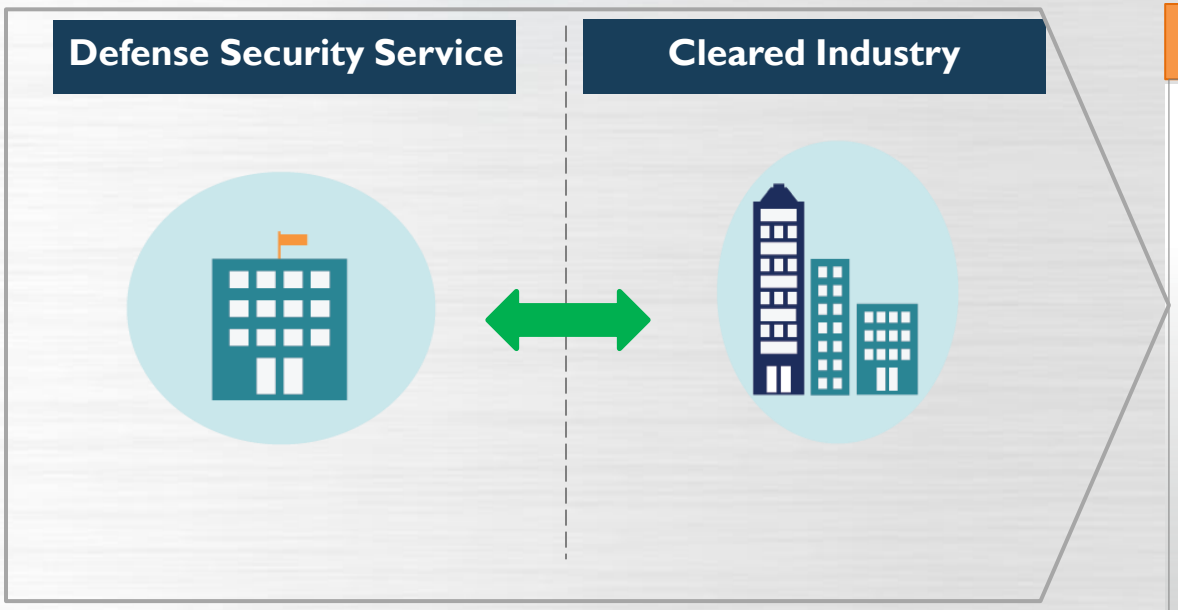
- *The Government Pays For Decisive Advantage Against Our Adversaries*
- *Companies Thrive due to the Advantages of Their Defense and National Security Platforms and Systems*
- *Our Public - Private Partnership is Expected to Maintain U.S. Advantage in Defense and National Security*
- *Together We Need to be Proactive Against The Threat - Forward Leaning*

DSS - Industry Partnership Critical

- **Partnership … key to continued success**

AS IS

Industry develops and creates technology on behalf of the government and government demands security



GOAL

* Industry recognizes it has primary accountability for securing assets & engages actively & demands government support

Pathway to Optimized Operational Impact

* **ASSUMPTION:** Industry has primary accountability/responsibility

Industrial Security Update

- DoD Insider Threat Management and Analysis Center
- Insider Threat Implementation…Conforming Change 2
- E.O.13691 Promoting Private Sector Cybersecurity Information Sharing
  - DHS…Cognizant Security Agency
- DTM 15-002…Policy Guidance for Processing of National Interest Determination
- Oversight of Industry Clearances
- FSO Effectiveness

POLICY UPDATES

Keith Minard, Acting Chief, Policy Division
Industrial Policy & Programs

NISP Contract Classification System (NCCS)

- What is NCCS? NCCS is:
  - an automated web based system created to facilitate the querying of DD 254 data and the management of security classification specification information
  - a coordinated effort between OUSD(AT&L) and DSS to provide a DoD and Federal enterprise solution for the creation, review, certification, and management of DD254's
  - Being built as an application on the DoD Wide Area Work Flow (WAWF) e-Business Suite Module
- What does it do?
  - Provides for more comprehensive NISP oversight
  - Creates a single, centralized, and secure repository for all DD254
  - Provides an integrated solution for DoD and Federal agencies in managing their classified contracts
- Testing and Timelines?

Implementation of Insider Threat in Cleared Industry

- When issued NISPOM Conforming Change 2 will require cleared industry to implement insider threat programs
- Industry has six-months to implement upon issuance of the NISPOM Conforming Change 2
- The NISPOM will outline minimum standards that include;
  - Establish and maintain an insider threat program
  - Designate insider threat senior official
  - Gather, integrate, and report
  - Conduct of self-assessments of insider threat program
  - Insider threat training
  - Monitoring network activity
  - User acknowledgements
  - Classified Banners

Implementation of Insider Threat in Cleared Industry

- To assist industry in implementing their Insider threat programs DSS:
  - Will issue additional clarification in an Industrial Security Letter
  - Will communicate to industry to inform them of the requirements
  - Is briefing insider threat program requirements at assessment exit briefs
  - Is updating the ODAA process manual to clarify IT related requirements in coordination with the NISPPAC Certification and Accreditation Working Group
  - Developing an insider threat job aid
  - Revising the industry self-assessment guide
  - Will be hosting web based online information sessions to provide additional information and clarification on program requirements
  - Internally coordinating oversight efforts of contractor insider threat programs

NATIONAL INTEREST DETERMINATIONS

Lynda Mallow, Acting Director
Industrial Policy & Programs

National Interest Determinations (NIDS)

- Directive Type Memorandum (DTM) 15-002, "Policy Guidance for the Processing of NIDS in Connection with Foreign Ownership, Control, or Influence (FOCI) was published on February 11, 2015
- The Director, DSS proposes NIDs on behalf of the DoD GCAs if a U.S. contractor will require access to proscribed information under a special security agreement (SSA)
- Where the NID does not require approval from a controlling agency for access to COMSEC, SCI, or RD the NID becomes final 30 days after DSS notifies the affected GCA unless the GCA does not concur
  - DSS will ensure continued communication with the GCA through the process to ensure a mutually agreeable solution is in place
- Access to proscribed information under the classification or jurisdiction of a USG agency other than the GCA will not be granted without the concurrence of the responsible USG control agency

National Interest Determinations (NIDS)

- Implementation
  - Communication to the NISP Community
    - The NID DTM issuance was discussed at the February 18, 2015 Government Industrial Security Working Group (GISWG)
    - On February 13 and 27 DSS hosted an overview and presentation on Defense Connect Online
    - Internet Postings
    - Update to be provided at next GISWG scheduled for April 29, 2015
  - Development of Processes
  - Timelines
- What does DSS need from you?
- What will you get from DSS?
- Where to send NID requests
  - NID@DSS.MIL

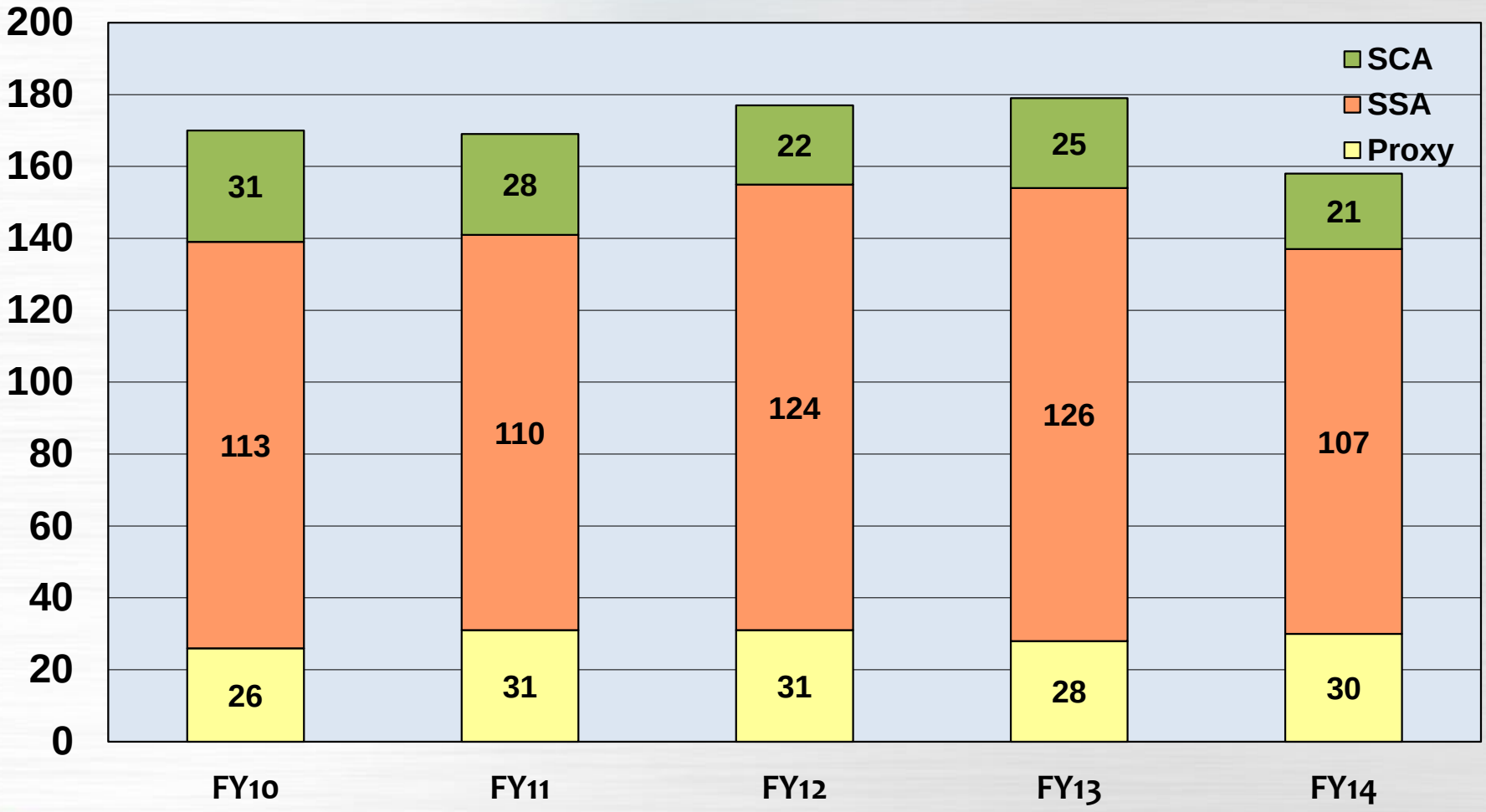
FOCI UPDATE

Nicoletta Giordani
Branch Chief, FOCI Operations Division

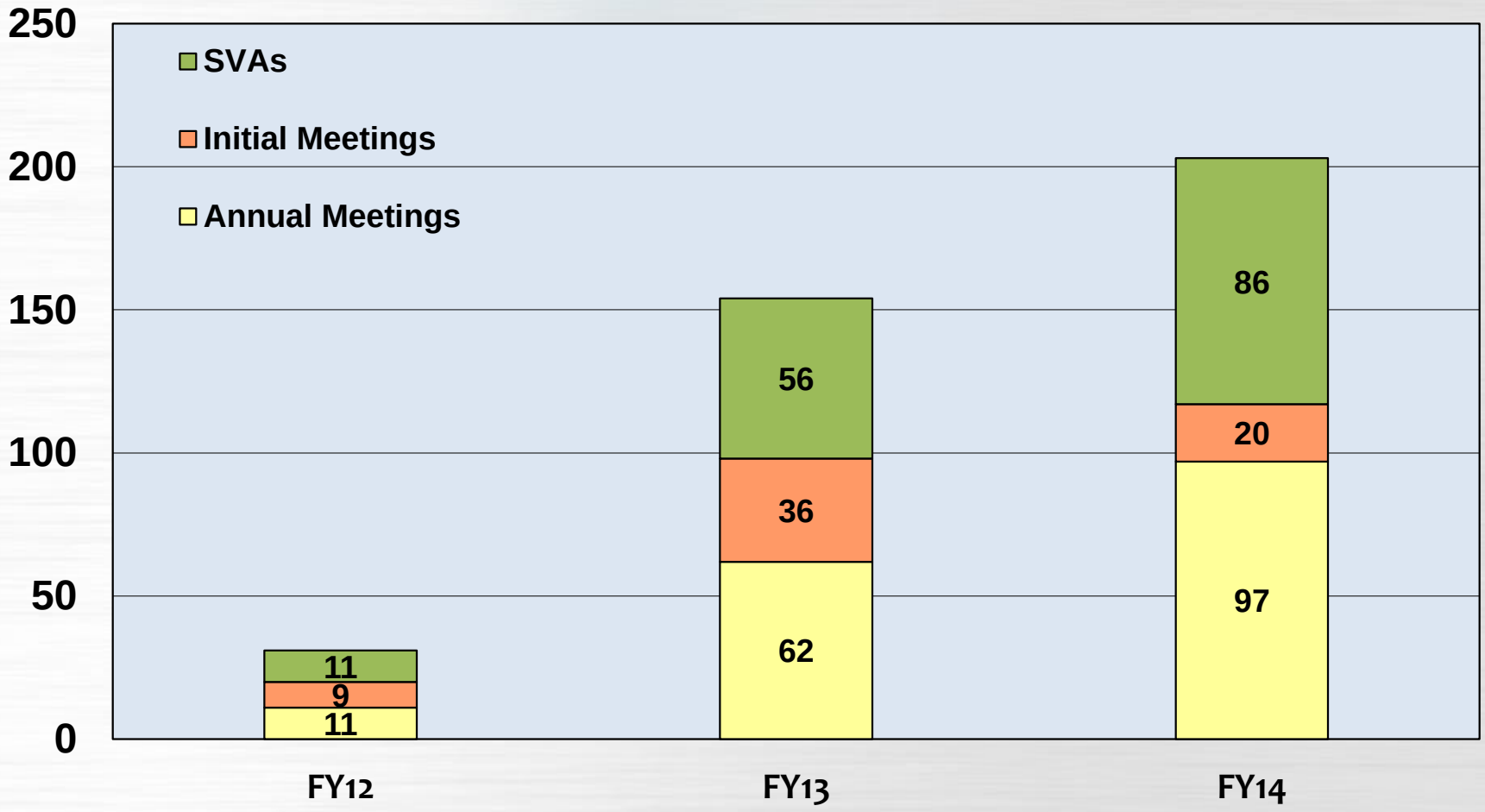
Agenda

- Numbers:
  - FOCI Numbers Year-Over-Year
  - Oversight
- Updates
- AOP Guidance
- Next Steps

Numbers – FOCI Agreements



Numbers – Oversight



Updates

- OD/PH Training available on DSS website
  - Three modules:
    - Module 1: Intro to DSS and FOCI
    - Module 2: Managing FOCI Mitigation
    - Module 3: Managing Relationships with FOCI Affiliates
  - In the process of developing three additional modules:
    - Module 4: Additional Responsibilities of the Proxy Holders and Voting Trustees
    - Module 5: Security Vulnerability Assessment
    - Module 6: Initial and Annual Compliance Meetings

Affiliated Operations Plan (AOP) Defined

- A document to capture relationships between the affiliates and mitigated entities, and find balance between security needs and business needs:
  - A **tool** for the GSC and DSS to provide transparency and assurance
  - Business enabler not a disrupter

- Often the most detailed governance document a FOCI company uses

- Defines broad categories of shared services:
  - Affiliated services (traditional and reverse)
  - Shared third party services*
  - Shared persons
  - Cooperative commercial arrangements*

*Does not require DSS pre-approval

AOP Elements

- For each service, the company is expected to provide:
  - **Description** of the service, including:
    - Who will provide service to whom and why?
    - What will be the frequency of interaction and how will it take place?
  - **Risks** inherent in sharing service and risk **mitigation** measures
    - FOCI Risks: lack of independence from affiliates and security risks
    - Mitigation Measures: processes implemented to prevent undue influence and/or unauthorized disclosure of classified or export controlled information
  - **Review** of the service, internally (GSC) and externally (DSS)
    - How will the GSC conduct oversight to ensure compliance? What role will the FSO and TCO play?
    - How will DSS ensure that the company is complying with the risk mitigation strategies outlined above? What can DSS review?

AOP - Common Misconceptions

- **"This service presents no FOCI risks"**
  - Sharing a service **always** presents FOCI risk, however unlikely, because any sharing allows the parent/affiliates to have a certain degree of leverage over the cleared company, thereby affecting the company's independence
- **"This service presents no risks because we have already mitigated them"**
  - Risks must be defined and mitigation measures should clearly demonstrate how they are structured to prevent identified risks
- **"Classified information is not at risk because ours is a non-possessing facility"**
  - There are many ways classified information can be compromised
- **"The Review section applies only to DSS review, not the GSC"**
  - The Review section shows how the GSC will conduct oversight of each service

AOP Examples of Risk/Mitigation

Service	Risk	Mitigation
Internal Audit	– Undue influence over FOCI entity operations and management – Unauthorized access to classified, export controlled, and/or sensitive/proprietary data	✓ FOCI entity or third party provider conducts audit ✓ Affiliates may provide specific scope of audit ✓ Audit results reviewed by GSC before released to affiliates
Human Resources	– Identify cleared employees and classified programs – Influence over hiring, firing, performance appraisals, and compensation	✓ PCL information managed by FOCI entity through FSO ✓ FOCI entity controls hiring, firing, performance appraisals, and compensation
Legal Services	– Influence over FOCI entity business, management, and/or legal decisions – Inadvertent disclosure of PCL information or classified, export controlled	✓ FOCI entity maintains a General Counsel ✓ Affiliate may provide specific guidance ✓ Separate engagement letters required when using third-party firm
Information Technology (IT)	– Unauthorized access to classified, export controlled, and/or sensitive/proprietary data – Maintain control over network/information	✓ FOCI entity maintains control over IT infrastructure through an approved ECP (physical and virtual separation) ✓ FSO/TCO and GSC review of IT networks, tools, and information shared while interfacing with Affiliates ✓ Only allow for push relationship

AOP - The Way Forward

- DSS will make available an AOP Guidance Document to Industry:
  - Identify potential and existing affiliated operations
  - Identify associated risks and develop risk mitigation measures
  - Describe affiliated operations within AOP to obtain DSS approval
  - Prepare for SVA
  - Best practices and discuss role of GSC/FSO/TCO
- DSS will make available a sample AOP to Industry
  - A redacted, approved AOP to help give life to the template

Next Steps

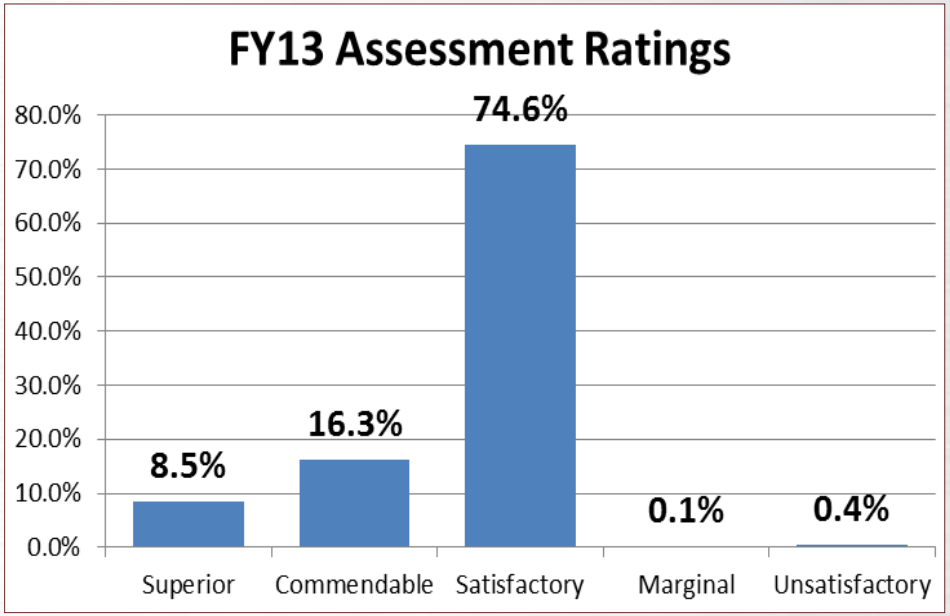
- AOP Guidance: DSS will make available an AOP Guidance Document and a sample AOP to Industry
- Annual Compliance Report: Provide more guidance to industry on how, when or what to submit for an Annual Compliance Report
- Due diligence guidance: DSS does not have any guidance to industry regarding requirements to protect classified and sensitive information during M&As
- Possible shift Third-party Relationships and Commercial Teaming Arrangements to the Annual Compliance Report
- Simplification of AOP/ECP/FLP to reduce overlap

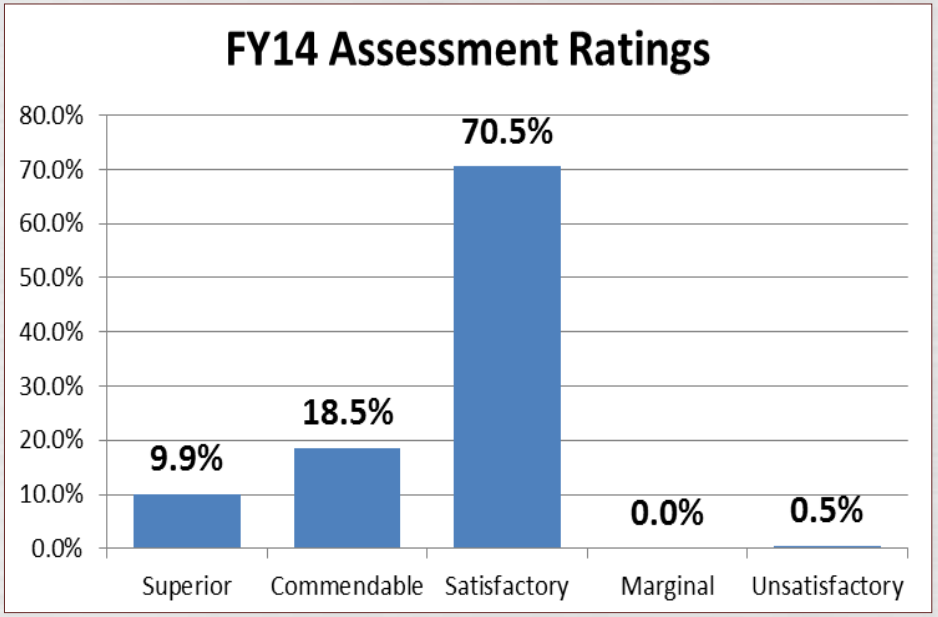
NISP OVERSIGHT AT FOCI COMPANIES

Heather Sims

Assistant Deputy Director for Industrial Security

What We're Finding





FOCI Oversight Data

- FY 2014, DSS has conducted 6,912 security vulnerability assessments.
  - 402 of which were under FOCI mitigation

- FOCI Compliance Breakdown:
  - 26% rated Superior
  - 31% rated Commendable
  - 42% rated Satisfactory
  - 2% rated Unsatisfactory

- National Compliance Breakdown:
  - 10% rated Superior
  - 19% rated Commendable
  - 70% rated Satisfactory
  - 1% rated Marginal/Unsatisfactory

Top Ten Common Vulnerabilities

1.	Inadequate security education, training, awareness	15.9%
2.	Persons without proper eligibility accessing classified	15.8%
3.	Not Auditing and reviewing audit results for classified systems	6.5%
4.	Failure to provide written notification that review of the SF-86 is for adequacy and completeness or destroy when eligibility has been granted or denied	5.7%
5.	Failure to perform self-inspection of security program	2.9%
6.	Not reporting classified compromises	2.4%
7.	Classified IS configuration and connectivity management	2.3%
8.	Personnel clearance re-investigations out-of-scope	2.2%
9.	Processing classified on an unaccredited computer system	2.1%
10.	Unreported facility clearance change conditions (foreign buyout, mergers, key management personnel changes, etc.)	1.8%

Purple = IT systems
Light Blue=Personnel Security Clearance
Dark Blue=Other process/procedures

FOCI Best Practices

- Frequent interaction with assigned Industrial Security Representative
- Effective /Proactive Approach to Monitoring Electronic Communications
- Self-Assessment of Facilities-High frequency and cross-pollination
- Solid Security Training & Education Program at all levels
- Active Participation in Security Community
- Government Security Committee Management Prerogative

Keys to Success

Management Support	*Active engagement and oversight by management personnel is vital to the success of a security program. Management should set overarching strategic objectives to ensure that all resources required to implement a robust security program is provided to the FSO or Security Program Manager.*
Security Education	*The hallmark of a successful security education program begins with it's flexibility. The program must be both dynamic and continuous; able to be applicable to both cleared and uncleared personnel. With continual management support this program can become part of the organizations culture versus a requirement of the NISP.*
Trained FSO, ISSM	*FSO and ISSM must adhere to the requirements of the NISPOM. Further training and enrichment should continue over the course of a security professionals career. Participation in the local security community via ISAC's or DSS programs like PWI is strongly encouraged.*
Security Integration Business Enterprise	*Security should be integrated into every part of your organization. Your HR, Finance and travel offices should be trained to recognize Adverse Information and other security concepts to serve as a force multiplier to your security office.*

Vulnerability Assessments

Focus Areas:

- Effectiveness of the FSO
- Personal Security Clearance Validation/Reduction
- Incident and Adverse Information Reporting